REMARKS

STATUS OF CLAIMS

Claim 5 has been amended. No claims have been added or withdrawn. Thus, Claims 1-7 are currently pending in the application.

SUMMARY OF THE REJECTIONS

Claim 1 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over U.S. Patent 6,088,803 by Tso et al. ("*Tso*") in view of U.S. Patent 5,937,150 by Phan et al. ("*Phan*"). Claims 2-3 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Tso* in view of *Phan* and in further view of U.S. Patent Publication 2003/0048468 A1 by Boldon et al. ("*Boldon*"). Claim 4-6 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Tso* in view of *Phan* and in further view of U.S. Patent Publication 2004/0025042 A1 by Kouznetsov et al ("*Kouznetsov*"). Claim 7 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Tso* in view of *Phan* and in further view of *Boldon*. The rejections are respectfully traversed.

It is respectfully submitted that each of the claims are patentable over the cited references for at least the reasons provided hereinafter.

CLAIM 1

Claim 1 recites:

"A multi-function peripheral device comprising:
a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;
a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;
one or more processors;
a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of the electronic document;
a print process executing in the memory and being configured to process print data and cause a printed version of an electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and
a virus protection process executing in the memory and being configured to perform the steps of:
detecting that a request for data to be analyzed for viral infection has been received by the multi-function peripheral device over the network from a network device; and
in response to detecting receipt of the request, causing the data to be provided from the multi-function peripheral device to the network device over the network to enable the data to be analyzed for viral infection at the network device." (Emphasis added.)

At least the above-bolded elements of Claim 1 are not anticipated by *Tso* in view of *Phan*, either alone or in combination. Claim 1 describes a multi-function peripheral device with a network interface that allows communication with other network devices in a network that also comprises, among other things, processes to perform scans, printing, and virus protection. Virus protection is important because multi-function peripheral devices, due to being connected to networks, are susceptible to viral infection. (*Written Specification*, par. [0005]). The bolded elements of Claim 1 describe virus protection for multi-function peripherals provided remotely via a network device. (*Written Specification*, par. [0018]).

Claim 1 features, among other things, "**detecting that a request for data to be analyzed for viral infection has been received by the multi-function peripheral device over the network from a network device; and in response to detecting receipt of the request, causing the data to be provided from the multi-function peripheral device to the network device over the network to enable the data to be analyzed for viral infection at the network device.**"

In Claim 1, the virus protection process detects that a request is received by the multi-function peripheral device for data to be analyzed for viral infection. Then, in response to detecting receipt of the request, the virus protection process "**caus[es] the data to be provided from the multi-function peripheral device to the network device over the network to enable the data to be analyzed for viral infection at the network device**." The "**response**" to the request is not merely "*causing the data to be provided…*," but rather that the data is being provided "**to enable the data to *be analyzed for viral infection* at the network device**."

As a result, in the approach of Claim 1, another device, namely "**a network device**," is performing the viral detection of the data that is ***provided from*** the multi-function peripheral device ***to*** the network device. This remote detection is initiated by the network device in the form of "a ***request*** for data **to be analyzed for viral infection**" with the multi-function peripheral device responding by sending the requested data so that the data may "***be analyzed for viral infection* at the network device**."

In particular, the Applicant notes that Claim 1 is supported in the Application at least by the embodiment described in Section VII. REMOTE VIRUS PROTECTION in paragraphs [0039-0045] and as illustrated in FIG. 4 and FIG. 5. Specifically, in step 502, MFP 402 receives a request from network device 404 for data to be tested for a viral infection, and in step 504, MFP 402 responds to the request by sending the requested data to network device 404 via network 406. Then in step 506, network device 404 performs virus testing on the data provided by MFP 402, such as by using virus protection tool 412. In step 508, network device 404 provides instructions to MFP 402 when the results of the virus testing show that the data is infected, such as network device 404 instructing MFP 402 to replace the data that was sent,

quarantine the infected data, or to delete the infected data. Then in step 510, MFP 402 performs the actions based on the instructions from network device 404 and provides notifications, if appropriate.

The Office Action states that *Tso* discloses "a network device configured with a virus scanner, the network device will intercept content send [sic] to a client device and scan the content for viral infection before the content reaches the client device on the network. (col. 2, lines 37-61; col. 3, line 1-38)." (*Office Action*, p. 2) However, this statement in the Office Action misstates the features of Claim 1 because the *network device intercepts content* sent to a client device (or MFP) and is *not a request made to the client device* (or MFP) for *data on the client device*. Furthermore, the *request does not originate from the network device*.

Claim 1 recites "**detecting that a request for data to be analyzed for viral infection has been received by the multi-function peripheral device over the network from a network device".** *Tso* fails to teach or disclose this limitation anywhere within the reference. Rather, *Tso* states "As shown in FIG. 2, processing begins upon receipt of a request for a data object from client device 1 (Step 20). Such a request may comprise, for example, an HTML (HyperText Markup Language) request specifying a particular URL (Uniform Resource Locator) associated with a Web page resident on content server 7. Network device 4 then retrieves the requested data object from content server 7, generally in the form of an HTML file (Step 30). Once the file is completely received, network device 4 invokes virus checker 5, which in turn performs its preconfigured virus scan processing with the requested file as input (Step 40)." (*Tso*, col. 2, line 61- col. 3, line 5). In *Tso*, a client device requests data from another source (content server 7), and *data from the content server is intercepted* by network device before reaching the client device. This is far different from the limitation recited in

Claim 1 where a network device makes a request to the MFP for data to be analyzed. Thus, in Claim 1, the virus scanning is selective, and is performed in response to a request. In *Tso*, no selective scanning is performed and all intercepted data is scanned. Selective scanning, or scanning performed in response to a request, is beneficial in situations where it is known that virus scanning is not necessary, e.g., data that has already been scanned, or data where virus scanning is not required.

The virus protection process in the MFP, upon detecting receipt of the request, then *provides data from the MFP to the network device* to enable the data to be analyzed for viral infection at the network device. Thus, not only does *Tso* fail to teach or suggest the limitation that a request is detected at the MFP from a network device to analyze data, but the limitation of data sent from the MFP to the network device to be analyzed is also clearly not taught. The other cited sections of *Tso* describe the setup of the network with a virus checker (*Tso*, col. 2, lines 37-61) and an alternate embodiment wherein the virus checker analyzes data from the content server as the data is received from the content server and not after the entire data is received (*Tso*, col. 3, lines 11-38).

The Office Action does not explain why those limitations are not shown in *Tso*, but instead offers the explanation "Examiner notes that the prior art provides a more advantageous virus detection system than the claimed invention. The claimed invention as disclosed provides a system for viral detection within the network, wherein devices (ie. MFP) within the network would receive viral infected content and distribute the viral infected content to other devices on the network without first examining the content for malware." (*Office Action*, p. 2). In effect, the Office Action admits that the data analyzed for viruses is not data on the MFP, as stated in Claim 1, but is data from another source that is entering the network. With

respect to the explanation, a perception of greater advantage is not relevant, only whether the cited art teaches or discloses the limitations recited in Claim 1. In this instance, the explanation clearly fails to show that *Tso* teaches or suggests the limitations in Claim 1 and only states that a different method, not containing the limitations of Claim 1, is advantageous. As such, at least one limitation has not been anticipated by *Tso* and Claim 1 should be allowable.

The Office Action relies upon *Phan* as allegedly disclosing a multi-function peripheral device that comprises "a network interface…a graphical user interface…a memory…a scan process…a print process…," and thus the Office Action does not rely upon *Phan* as disclosing any of the features of Claim 1 that the Office Action relies upon as being disclosed in *Tso*. Nevertheless, the Applicant has reviewed *Phan* and yet found nothing in *Phan* related to the features of Claim 1 discussed above.

In addition, while the Office Action does not rely upon *Kouznetsov* in the rejection of Claim 1, and instead uses this reference in the rejections of other claims, the Applicant can similarly find nothing in *Kouznetsov* related to the features of Claim 1 discussed above.

Because *Tso*, *Phan*, and *Kouznetsov*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "**detecting that a request for data to be analyzed for viral infection has been received by the multi-function peripheral device over the network from a network device; and in response to detecting receipt of the request, causing the data to be provided from the multi-function peripheral device to the network device over the network to enable the data to be analyzed for viral infection at the network device**," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

CLAIM 4

Regarding Claim 4, the Office Action states that *Kouznetsov* discloses "receiving replacement data for the multi-function peripheral (paragraph 0161, lines 1-2; paragraph 0169, lines 1-2)." As a preliminary administrative matter, Claim 4 includes additional features that are not even addressed in the rejection of Claim 4 in the Office Action. Specifically, Claim 4 does not only feature "receiving replacement data for the multi-function peripheral, but Claim 4 also features "receive replacement data from the network device that has been disinfected" and "replace the data on the multi-function peripheral device with the replacement data." Thus, it appears to the Applicant that the rejection of Claim 4 based on *Kouznetsov* is incomplete because several additional features of Claim 4 are not addressed in the rejection.

Nevertheless, the Applicant respectfully submits that *Kouznetsov* fails to disclose the features of Claim 4, for at least the reasons given herein. First, the cited portion from paragraph [0161] states in its entirety: "A clean record contains a function for removing the malware and repairing files, if possible." While this disclosure may be interpreted as describing the disinfecting of a file that is infected with "malware," there is nothing in this disclosure or elsewhere in *Kouznetsov* that the Applicant has found about a multi-function peripheral device that can "receive replacement data from the network device that has been disinfected." The Applicant notes that this network device being referred to therein in Claim 4 is the same network device as in Claim 1 (from which Claim 4 depends), and that in Claim 1, that network device both (a) "sent the request [to the multi-function peripheral device] for data to be analyzed for viral infection" and then (b) after the data is "provided

from the multi-function peripheral device to the network device," thereby enable[s] the data to be analyzed for viral infection at the network device."

Second, paragraph [0169] is given as disclosing the limitation, but paragraph [0169] merely introduces the logged events of Table 17. It appears to the Applicant that the Office Action may have intended to cite to paragraph [0165] rather than paragraph [0169], since that paragraph includes the word "replacing" that is similar to the term "replace" used in Claim 4. But again, that explanation by *Kouznetsov* that replacing a record is the same as deleting a record and adding a new record is not the same as replacement data that has been disinfected, as in Claim 4, little less that such replacement data is received by the multi-function peripheral device from the network device or that the multi-function peripheral device replaces the data with the replacement data. In fact, paragraph [0165] appears to be nothing more than an explanation that a record is replaced by deleting the record and adding a new record in place of the deleted record, whereas in Claim 4, the replacement data is disinfected by the network device, not merely deleted.

In summary, because *Tso*, *Phan*, and *Kouznetsov*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "receive replacement data from the network device that has been disinfected" and "replace the data on the multi-function peripheral device with the replacement data," the Applicant respectfully submits that, for at least the reasons stated above, Claim 4 is allowable over the art of record and is in condition for allowance.

CLAIM 7

Regarding Claim 7, the Office Action states that *Boldon* discloses "receive a request from the network device for the multi-function peripheral to quarantine or delete at least a

portion of the data that was sent from the multi-function peripheral device to the network device (paragraph 0023, lines 1-5)." However, as discussed above, paragraph [0023] of *Boldon* merely explains that the printing device, upon detecting a virus in the information to be printed, deletes the information and/or contacts a system administrator, so as to eliminate the virus or at least prevent the spread of the virus to other printing devices and general-purpose devices. (Paragraph [0023].) While this portion of *Boldon* does describe the deletion of information that is detected has having a virus, the features of Claim 7 being rejected based upon this portion of *Boldon* do not merely include "delete at least a portion of the data that was sent…."

Instead, the relevant features of Claim 7 are that the multi-function peripheral device is configured to perform the step of "**receive a *request*** from a network device…." and that that request is for the "multi-function peripheral device to quarantine or delete a portion of the data…" Recall that in Claim 1, from which Claim 7 depends, the analysis of the data for viral infection is not performed by the multi-function peripheral device, but rather the analysis for viral infection is performed at the network device that requests the data being analyzed to be provided to the network device by the multi-function peripheral device. Thus, in Claim 7, it is the network device that requests that the multi-function peripheral device quarantine or delete the portion of the data that was sent via the steps of Claim 1. This is consistent with Claim 1 being an approach for the network device to detect a viral infection in data requested from the multi-function peripheral device, and thus the network device requests that the multi-function peripheral device act to deal with the viral infection by either quarantining or deleting at least a portion of the data that has the viral infection.

Also regarding Claim 7, the Office Action states that *Boldon* discloses "[in] response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the network device (paragraph 0006, lines 4-7; paragraph 0007, lines 4-7; paragraph 0016, lines 5-14." However, these cited portions of *Boldon* again do not disclose anything about a multi-function peripheral receiving "**a *request*** from a network device…." and that such a request is for the "multi-function peripheral device to quarantine or delete a portion of the data…," as featured in Claim 7.

Specifically, the latter portion of paragraph [0006] of *Boldon* describes forwarding information to a printing device that scans the information to see if the information contains a virus, and printing the information if no virus is detected. But this says nothing about a multi-function peripheral receiving "**a *request*** from a network device…." and that that request is that the "multi-function peripheral device to quarantine or delete a portion of the data…," as featured in Claim 7.

Also, the latter portion of paragraph [0007] of *Boldon* describes that *Boldon's* approach includes deleting the information if it contains a virus and/or contacting a system administrator if a virus is found. But again, this says nothing about a multi-function peripheral receiving "**a *request*** from a network device…." and that that request is that the "multi-function peripheral device to quarantine or delete a portion of the data…," as featured in Claim 7.

Finally, the latter portion of paragraph [0016] of *Boldon* describes, as discussed above, that modern peripherals have greatly expanded functionality, including acting as file servers to keep certain files internally and to send them to other devices when requested, receiving data

in the form of programming language to be used to implement new functionality at the peripheral to change the way the device performs its job, and sending data to other devices based on any number of criteria. (Paragraph [0016].) While this paragraph uses the word "requested," it is in the context of the peripheral sending a file stored at the peripheral when the peripheral is acting as a file server, but such a request is not "**a *request*** from a network device…." and that that request is that the "multi-function peripheral device to quarantine or delete a portion of the data…," as featured in Claim 7.

In fact, the purpose of *Boldon's* approach is for the printer to scan print jobs for viruses and for the printer to then deal with any that are found, and therefore, there is no reason for *Boldon's* approach to include that some other device besides the printer would request that the printer quarantine or delete the information that the printer detects as having a virus. Rather, *Boldon* merely discloses that the printer scans a print job, and if a virus is found, deletes the print job and/or contacts a system administrator, and there is nothing in these cited portions of *Boldon* or elsewhere about *Boldon's* printer acting upon a print job in which the printer has detected a virus based upon a request from another device to take such a particular action that is specified by the other device to Boldon's *printer*.

In summary, because *Boldon*, *Tso*, *Phan*, and *Kouznetsov*, either alone or in combination, fail to disclose, teach, suggest, or in any way render obvious "receive a request from the network device for the multi-function peripheral to quarantine or delete at least a portion of the data that was sent from the multi-function peripheral device to the network device" and "in response to receiving the request from the network device to quarantine or delete at least a portion of the data that was sent to the network device, quarantine or delete the at least a portion of the data that was sent from the multi-function peripheral device to the

network device," the Applicant respectfully submits that, for at least the reasons stated above, Claim 7 is allowable over the art of record and is in condition for allowance.

CLAIMS 2-3 and 4-6

Claims 2-3 and 4-6 are dependent claims, each of which depends directly on Claim 1 discussed above, and thus include each and every feature of the corresponding independent Claim. Each of Claims 2-3 and 4-6 is therefore allowable for the reasons given above for Claim 1. In addition, each of Claims 2-3 and 4-6 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time, although the Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims. Therefore, it is respectfully submitted that Claims 2-3 and 4-6 are allowable for the reasons given above with respect to Claim 1.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. Entry of the amendments and further examination on the merits are respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

/RobertSChee#58554/
Robert S. Chee Reg. No. 58,554

Date: February 14, 2008

2055 Gateway Place, Suite 550
San Jose, CA 95110-1083
Telephone: (408) 414-1080
Facsimile: (408) 414-1076